

12/15/99
CLP
Case No. 123456789

12-16-99
12

Case Docket No. PHA 23,890

THE COMMISSIONER OF PATENTS AND TRADEMARKS, Washington, D.C. 20231

Enclosed for filing is the patent application of Inventor(s):
JIN LU AND MARTIN FREEMAN

For: SYSTEM AND METHOD FOR COPY PROTECTING TRANSMITTED INFORMATION

Jc511 U.S. PTO
09/461984
12/15/99

ENCLOSED ARE:

- Associate Power of Attorney;
- Information Disclosure Statement, Form PTO-1449 and copies of documents listed therein;
- Preliminary Amendment;
- Specification (19 Pages of Specification, Claims, & Abstract);
- Declaration and Power of Attorney:
(3 Pages of a fully executed unsigned Declaration);
- Drawing (3 sheets of informal formal sheets);
- Certified copy of application Serial No. ;
- Other: ;
- Assignment to PHILIPS ELECTRONICS NORTH AMERICA CORPORATION.

FEE COMPUTATION

CLAIMS AS FILED				
FOR	NUMBER FILED	NUMBER EXTRA	RATE	BASIC FEE - 760.00
Total Claims	17 - 20 = 0		X \$18 =	0.00
Independent Claims	4 - 3 = 1		X \$78 =	78.00
Multiple Dependent Claims, if any			\$260 =	0.00
TOTAL FILING FEE =				\$838.00

Please charge Deposit Account No. 14-1270 in the amount of the total filing fee indicated above, plus any deficiencies. The Commissioner is also hereby authorized to charge any other fees which may be required, except the issue fee, or credit any overpayment to Account No. 14-1270.

Amend the specification by inserting before the first line the sentence: --This is a continuation-in-part of application Serial No. , filed ---.

CERTIFICATE OF EXPRESS MAILING

Express Mail Mailing Label No. EL335550770US

Date of Deposit December 15, 1999

I hereby certify that this paper and/or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Josephine Cangeleri
Typed Name Josephine Cangeleri
Signature

Daniel J. Piotrowski, Reg. 42,079

Attorney

(914) 333-9633

U.S. Philips Corporation

580 White Plains Road

Tarrytown, New York 10591

S:PW\MP09PW10.CNO

SYSTEM AND METHOD FOR COPY PROTECTING TRANSMITTED
INFORMATION

Field of the Invention

5 This invention relates to a communication system and, more particularly, to a copy protection system for information transmitted between a deployment module, such as a point of deployment (POD) module, and a host device, such as a set-top box.

10

Background of the Invention

Digital video and audio consumer electronics/devices are used by consumers to receive and conduct numerous services and transactions, for example, to receive video, 15 audio and data streams from a (cable television) service provider, such as Emergency Alerting, Interactive Program Guides, Impulse Pay-Per-View (IPPV), Video On Demand (VOD), General Messaging, and Interactive Services.

In particular, one such device is a point of 20 deployment (POD) module. A POD module is a removable card inserted into a host device, such as a set-top box. As is well known in the art, a POD module provides several functions including security that is physically separate from a set-top box's navigation function and processing 25 out-of-band cable signals. For additional details on POD modules, see SOCIETY OF CABLE TELECOMMUNICATIONS ENGINEERS, INC. (SCTE) Document: SCTE DVS 131 Rev. 7, entitled "Draft Point-of-Deployment (POD) Module Interface Proposal" dated December 3, 1998, (hereinafter known as 30 "DVS131r7").

Consumers rely on such devices to communicate, access

programs and services or engage in commercial transactions in which privacy and/or security is desired and, in many cases, expected. In this regard, the POD module also decrypts content information encrypted by service providers. It may be part of a so-called "conditional access" (CA) system that spans the head-end of a service provider network and the POD module itself.

To receive information from a particular service provider, a POD module that contains an algorithm related to a particular proprietary CA system, which is associated with a particular service provider, must be inserted to a host device. After content information is selected by the host device/viewer and received in the POD module from a service provider, it is decrypted in the POD module. The (decrypted) content information is again encrypted in the POD module with a new set of keys to protect it when transmitted across the POD/host interface.

The content information is transmitted in a so-called transport stream, which contains several elementary streams. An elementary stream may contain a video feed, a sound track or a data file. Copy protection is provided on the basis of elementary streams.

For every copy protected elementary stream, there is an associated Copy Control Information (CCI). It is used by the host device to decide (1) how many copies (e.g. one copy, zero copies) of the elementary stream can be made; (2) what copy formats are allowed (e.g. analog formats including composite and component and digital formats); and (3) other copy protection related activities. The CCI is passed from the POD module to the host device to indicate how the corresponding elementary stream of the

content should be treated. To prevent an "intruder" from tampering with the CCI, it must be protected when transmitted to the host device.

Standard cryptographic methods exist for the general 5 encryption/decryption within such a system, however, these methods each have significant limitations. In one such method a proprietary CA system, as well as its associated algorithms for encryption/decryption, is used. Instead of transmitting every CCI associated with an elementary 10 stream in the content, this method transmits the most restrictive CCI to the host.

Although, the CCI is not encrypted when transmitted between the POD module and the host device, it is afforded some degree of protection. The CCI is typically embedded 15 in shared keys that are used to encrypt the content information at the POD module and decrypt the content information when received by the host device.

One problem with this approach is that if the content contains multiple elementary streams, each elementary 20 stream may have a different CCI. Since the host device uses the most restrictive CCI for its copy protection processing, content information may be prevented from being properly copied. For example, if there are two elementary streams, and the CCI associated with the first 25 one indicates "copy once", while the CCI associated with the second one indicates "never copy", then neither of the elementary streams can be copied. This prevents a stream from being legally copied when another (possibly unrelated) stream has a more restrictive CCI.

30 Thus, there is a clear and present need for an effective means to provide copy protection that utilizes

encryption, while still providing consumers with the information desired in a less restrictive manner. In particular, copy protection of information between a POD module and a set-top box.

5

Summary of the Invention

The problems associated with copy protection of information, such as content information from a service provider, transmitted between a deployment module, such as 10 a POD module, and a host device, such as a set-top box, are reduced or overcome by an arrangement in accordance with the principles of the present invention in which at least one control information pair is associated with the transmitted copy protected information, for example, one 15 control information pair for each elementary stream relating to selected content information (e.g. a program from a cable service provider).

Specifically, the control information pair includes, in addition to copy control information (CCI), a stream 20 identifier. The stream identifier uniquely identifies the transmitted copy protected information (or portion thereof e.g. an elementary stream).

In particular, it is an object of the present invention to eliminate the use of the most restrictive 25 copy control information (CCI), when for example multiple content information or elementary streams are received by a deployment module.

In one illustrative embodiment, a Packet Identifier (PID) associated with each elementary stream of the 30 transmitted copy protected information is used as the stream identifier for the respective elementary stream. A

PID indicates the type of data stored in the packet payload. Preferably, the stream identifier is incorporated with the Packetized Elementary Stream (PES) header of the elementary stream. Since the PES header for copy 5 protected information is encrypted during transmission between the deployment module and host device, the stream-identifier is in turn protected.

To help prevent hackers or intruders from illegally manipulating the copy protected information, the control 10 information pair(s) is incorporated into shared (session) keys, which are generated respectively, on both the deployment module and the host device. Accordingly, if the control information pair(s) is tampered with, then the respective shared key(s) in the host and deployment module 15 will not match. As a result, the host device will not be able to correctly decrypt the copy protected information encrypted by the deployment module with its shared key(s), thereby thwarting an intruder's attempt at illegally manipulating the copy protected information.

20

Brief Description of the Drawing

The invention will be more readily understood after reading the following detailed description taken in conjunction with the accompanying drawing, in which:

25 FIG. 1 illustrates an exemplary system in accordance with the principles of the present invention; and

FIG. 2 is a flowchart depicting the process for copy protecting transmitted information in the system of FIG 1.

30

Detailed Description

FIG. 1 is an exemplary system according to the principles of the present invention in which copy protection for information transmitted from a deployment module to a host device is implemented. It will be recognized that FIG. 1 is simplified for explanation purposes and that the full system environment for the invention will comprise, for example, a cable, fiber or satellite service provider network or provisions for network reliability through redundancy, all of which need not be shown here. The system illustratively includes a host device 10, such as a set-top box, and a deployment module 12, such as a point of deployment (POD) module, which communicate with each other through a communication medium 14, for example, wireless communication, electromagnetic card interface, optical communication, and the like.

Deployment module 12 includes a host interface 16 and a processor 18. Host interface 16 is used to communicate with host device 10 via medium 14. Host interface 16 may be any conventional system for allowing the transmission of information between the host device and the deployment module. For example, medium 14 may include a standardized bi-directional access to Out-Of-Band RF and in-band MPEG-2 Transport Stream input and output device.

The majority of logic, control, supervisory, translation functions required for the operation of deployment module 12 is performed by processor 18 which also includes programs for the operations functionally described in FIG. 2. As described in detail below, execution of these program implements the functionality

necessary to copy protect information. Processor 18 can be any of a number of commercially available processors, for example that may include dedicated digital signal processors (DSPs), a central processing unit (CPU) and 5 memory chips.

Although deployment module 12 is described as a POD module, this arrangement is merely for convenience and it is to be understood that deployment modules are not limited to POD modules, per se. As used herein, the term 10 "deployment module" refers to any type of (1) point of deployment module, (2) wireless, cellular or radio data interface appliance, (3) smartcard (4) personal computer, and (5) internet interface appliance, which facilitates the transfer of data, access remote services or engage in 15 transactions and in which privacy and/or security is desired.

Host 10 communicates with deployment module 12 through communication medium 14. Host 10 includes a deployment module interface 24, which is arranged to 20 operate with host interface 16, a server provider interface 20 and a processor 22.

Similar to the deployment module, the majority of logic, control, supervisory, translation functions required for the operation of host 10 are performed by 25 processor 22 which also includes programs for the operations functionally described in FIG. 2. As described in detail below, execution of these programs implements the functionality necessary to copy protect information transmitted between a deployment module and a host. 30 Processor 22 can be any of a number of commercially available processors, for example that may include

dedicated digital signal processors (DSPs), a central processing unit (CPU) and memory chips.

The principles of the present invention are particularly useful for the copy protection of information 5 or data transmitted between a POD module and a host device in a service provider communications network, such as a cable television network. However, it is to be understood that the steps described below in FIG. 2 are equally applicable to other devices described above.

10 FIG. 2 is a flow chart showing the steps carried out within the system of FIG. 1 to implement copy protection of information transmitted between a deployment module and a host device according to the principles of the present invention. The operation of copy protection in such 15 communications networks is started by authenticating the host device using the deployment module.

With simultaneous reference to FIGS. 1 and 2, the process contemplated by the invention is initiated in step 200 of FIG. 2, when a host device, for example host 20 device 10 of FIG. 1, transmits a certificate to a service provider (not shown) for host device authentication. The certificate, for example, includes a host ID. Typically, this step is carried out during a deployment module initialization, for example, when deployment module 12 of 25 FIG. 1, is inserted into a card interface of host device 10 or host device 10 is powered up. If the certificate is not identified or is inconsistent with information at the service provider, then the host device is invalidated and the transaction is terminated. If the host device is 30 authenticated in step 202, the process proceeds to step 206.

In step 206, when particular (content) information is selected, the host device notifies the deployment module via a request message. The particular information is selected, for example, by a user selecting a channel on 5 cable television network. By looking at the electronic program guide (EPG), the host device determines which video, audio and/or data streams are contained in the selected information, for example, channel or programs. The request message also contains the PIDs of the 10 elementary streams associated with the selected information.

In step 208, the deployment module, after receiving the selected PIDs from the request message, prepares to decrypt the elementary streams identified by the PIDs and 15 then re-encrypt them for copy protection. Preparing the elementary stream decryption involves deriving session keys from a conditional access (CA) system, so that the deployment module can decrypt the selected information from the service provider. After this preparation is 20 complete, in step 210, a reply message is sent from the deployment module to the host device to indicate that the deployment module is ready to decrypt the associated streams from the service provider. Included in the reply message is at least one control information pair 25 associated with the selected information, and each pair having a stream identifier and a CCI.

Thereafter, in step 212, shared keys are calculated by the deployment module and host device, incorporating the control information pair(s), unlike the prior art that 30 used only a CCI. The shared keys are a pair of keys (for example even and odd keys) shared by both the deployment

module and the host device. Both the deployment module and the host device use the shared keys, respectively, to encrypt and decrypt information crossing the deployment module/host device interface. For the shared key 5 calculation any of a number of methods can be used, see for example, Cable Television Laboratories specification entitled "OpenCable™ POD Copy Protection System DRAFT REV 991008" Document: IS-POD-CP-WD02-991027, published on October 27, 1999, (hereinafter "IS-POD-CP"), which is 10 incorporated by reference herein. As is well known by persons skilled in the art, the shared key pair is a function of a number of factors, including random numbers, public keys exchanged between the deployment module and host device, and the Host ID.

15 Illustratively, the host device computes an ODD/EVEN key pair using a conventional hash function, for example, SHA-1 Secure Hash Algorithm (for further details on the SHA-1 hash function, see IS-POD-CP), where the control information pair(s) is represented by "streamer 20 identifier-cci":

```
ODDHost = SHA-1[NHost | streamer_identifier-cci| Ks | Kcpss]  
lsb56  
  
25 EVENHost = SHA-1[NHost | streamer_identifier-cci| Ks | Kcpss]  
msb56
```

The deployment module's CA module computes an ODD/EVEN key pair using the SHA-1 has function:

30 ODD_{CA_Module} = SHA-1[N_{Host} | N_{module} | streamer_identifier-cci| K_s
| K_{validated_cpss}] lsb56

5
EVEN_{CA_Module} = SHA-1[N_{Host} | N_{module} | streamer_identifier-cci |
K_s | K_{validated_cpss}] msb56

10 where N_{Host} and N_{module} are two random numbers generated on the host device and deployment module respectively, K_s and K_{cpss} are two generated keys, lsb56 refers to the least significant 56 bits and msb56 refers to the most significant 56 bits, and streamer identifier-cci is calculated as follows,

15 streamer identifier-cci = SHA-1[stream identifier₁|CCI₁ |
....| stream identifier_n| CCI_n]

where the stream identifier_i and CCI_i are the control information pair for elementary stream i.

In a preferred embodiment the stream identifier uniquely identifies an elementary stream and is inserted into the PES header associated with the elementary stream at the time a PID is assigned to the elementary stream. Preferably, this takes place in the head-end of the service provider network at the time a transport stream is generated from elementary streams. In particular, a 7-bit field in the PES header called "additional copy info" is available for copy protection, see International Telecommunication Union (ITU-T) Recommendation H.222.0 / ISO/IEC 13818-1 (1996-04), entitled "Information Technology - Generic Coding of Moving Pictures and Associated Audio Information: Systems," which is incorporated by reference herein. The additional copy

info field is used to store the stream identifier. A 7-bit number can support up to 128 different stream identifiers, which is typically enough for the number of copy protected elementary streams in one transport stream.

5 After the host device has decrypted the encrypted PES, the stream identifier is retrieved.

After the deployment module finishes its calculation of the shared session key(s), it sends a synchronization message to the host device to indicate that it is ready 10 to send the encrypted information to the host device, represented by step 214.

After the host device finishes its calculation of the shared session key(s), it synchronizes with the deployment module, and the deployment module transmits the encrypted 15 information, represented by step 216.

The host device then begins to decrypt the encrypted information (e.g. the selected copy protected content information that has been encrypted with the shared key(s)). Accordingly, host device 10 is allowed to 20 complete a transaction or receive the selected services.

For example, the host device changes to a selected program channel of a cable service provider. However, if the shared key(s) do not match (for example, due to an attempt to temper with the control information pairs), the 25 decryption of the copy protected content fails, for example, viewers will only receive scrambled information, such as scrambled pictures. These steps are represented by steps 218-222. Thereafter, the user can select new information by returning to step 206.

30 Advantageously, even if an interloper intercepts a transmission between the host device and deployment

module, he or she can not directly detect the stream identifier, since it is encrypted in the PES header. Thus, even if a CCI is detected, an interloper can not tamper with the selected information, for example, swap 5 the PID fields associated with two streams. The possibility of such remapping is substantially reduced, since the stream identifiers are bound to their associated elementary streams and this binding is protected by encryption.

10 Finally, it is to be understood that although the invention is disclosed herein in the context of particular illustrative embodiments, those skilled in the art will be able to devise numerous alternative arrangements. Such alternative arrangements, although not explicitly shown or 15 described herein, embody the principles of the present invention and are thus within its spirit and scope.

Claims:

1 1. A system for copy protecting information, the
2 system comprising:
3 a point of deployment module; and
4 a set-top box including;
5 wherein the set-top box transmits a request message
6 for information, the point of deployment module generates
7 a reply message which includes at least one control
8 information pair, relating to the information, each
9 control information pair having copy control information
10 and a stream identifier, respectively generating a first
11 in the point of deployment module and a second key in the
12 set-top box, using the at least one control information
13 pair, and the point of deployment module encrypting the
14 information with the first shared key and transmitting the
15 encrypted information to the set-top box, and the set-top
16 box decrypting the encrypted information with the second
17 shared key when the first and second shared keys match.

18

1 2. A method of copy protecting information
2 transmitted between a deployment module and a host device,
3 the method comprising the steps of:
4 (a) transmitting a request message for the
5 information from the host device to the deployment module;
6 (b) transmitting a reply message from the deployment
7 module to the host device, wherein the reply message
8 includes at least one control information pair, each pair
9 having a copy control information and a stream identifier;
10 (c) generating a first shared key at the host and a
11 second shared key at the deployment module, respectively,

12 using the at least one control information pair and an
13 encryption means;

14 (d) encrypting, in the deployment module, the
15 information;

16 (e) transmitting the encrypted information from the
17 deployment module to the host;

18 (f) decrypting, at the host, the encrypted
19 information; and

20 (g) receiving the information at the host when the
21 first and second shared keys match.

22

1 3. The method of claim 2, wherein the deployment
2 module is a point of deployment module.

3

1 4. The method of claim 2, wherein the host is a set-
2 top box.

3

1 5. The method of claim 2, wherein the encryption
2 means includes a hash function.

3

1 6. The method of claim 2, wherein the encrypted
2 information in an elementary stream of information is
3 encrypted with the first shared key.

4

1 7. The method of claim 6, wherein the stream
2 identifier that is transmitted to the host is incorporated
3 with the Packetized Elementary Stream (PES) header of the
4 elementary stream.

5

1 8. A deployment module for use with a host device,
2 the deployment module comprising:

3 means for communicating with the host device; and
4 a processor for, in response to a request message for
5 information from the host device, generating a reply
6 message to the host device, the reply message including at
7 least one control information pair, each pair having copy
8 control information and a stream identifier, generating a
9 first shared key using the at least one control
10 information pair, encrypting the information with the
11 first shared key and transmitting the encrypted
12 information to the host device.

13

1 9. The deployment module of claim 8, wherein the
2 deployment module is selected from the group consisting of
3 a point of deployment module, wireless data interface
4 appliance, smartcard, personal computer or internet
5 interface appliance.

6

1 10. The deployment module of claim 9, wherein the
2 host device is a set-top box.

3

1 11. The deployment module of claim 10, wherein the
2 encrypted information is transmitted to the host device
3 using a transport stream, wherein the transport stream
4 includes at least one elementary stream.

5

1 12. The deployment module of claim 11, wherein
2 respective ones of the at least one control information
3 pairs is associated with respective ones of the at least
4 one elementary streams.

5

1 13. A host device for use with a deployment module,

2 the host device comprising:

3 means for communicating with the deployment module;

4 and

5 a processor for generating a request message for
6 information to the deployment module, and in response,
7 receiving a reply message from the deployment module,
8 wherein the reply message includes at least one control
9 information pair, each pair having copy control
10 information and a stream identifier, generating a second
11 shared key using the at least one control information
12 pair, and decrypting encrypted information, received from
13 the deployment module, with the second shared key, and
14 receiving the information when the second shared key
15 matches a first shared key generated in the deployment
16 module.

17

1 14. The host device of claim 13, wherein the
2 deployment module is selected from the group consisting of
3 a point of deployment module, wireless data interface
4 appliance, smartcard, personal computer or internet
5 interface appliance.

6

1 15. The host device of claim 14, wherein the host
2 device is a set-top box.

3

1 16. The host device of claim 13, wherein the received
2 encrypted information is included in a transport stream,
3 wherein the transport stream includes at least one
4 elementary stream.

5

1 17. The deployment module of claim 16, wherein

2 respective ones of the at least one control information
3 pairs is associated with respective ones of the at least
4 one elementary streams.

5

ABSTRACT

Method and system for copy protecting information from a service provider, which is transmitted between a point of deployment (POD) module and a set-top box, are disclosed by an arrangement in which control information pairs are transmitted from the POD module to the set-top box. The control information pairs are respectively associated with the portions of the copy protected information, for example, elementary streams, transmitted between the POD module and host device. To prevent hackers or an intruder from tampering with the copy protected information, the control information pairs are incorporated into a shared key calculation in the POD module and set-top box. The shared keys are used by the POD module and set-top box to encrypt and decrypt the information (e.g. elementary streams). If the at least one control information pair is tampered with during transmission between the POD module and the set-top box, then the shared key(s) calculated by the set-top box and POD module will not match, and the set-top box will not be able to correctly decrypt the encrypted information received from the deployment module.

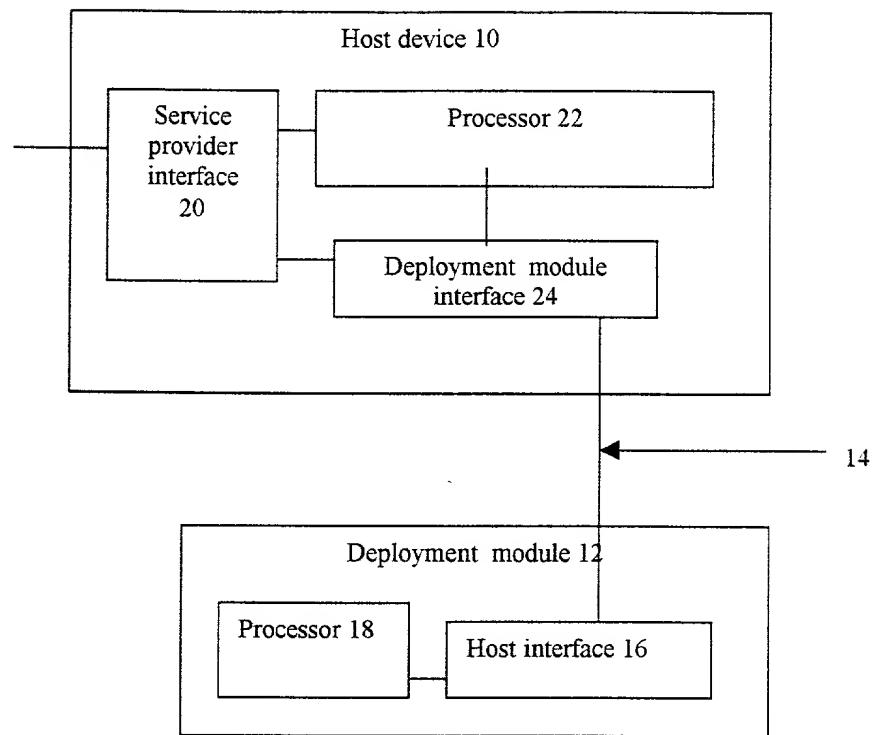


FIG. 1

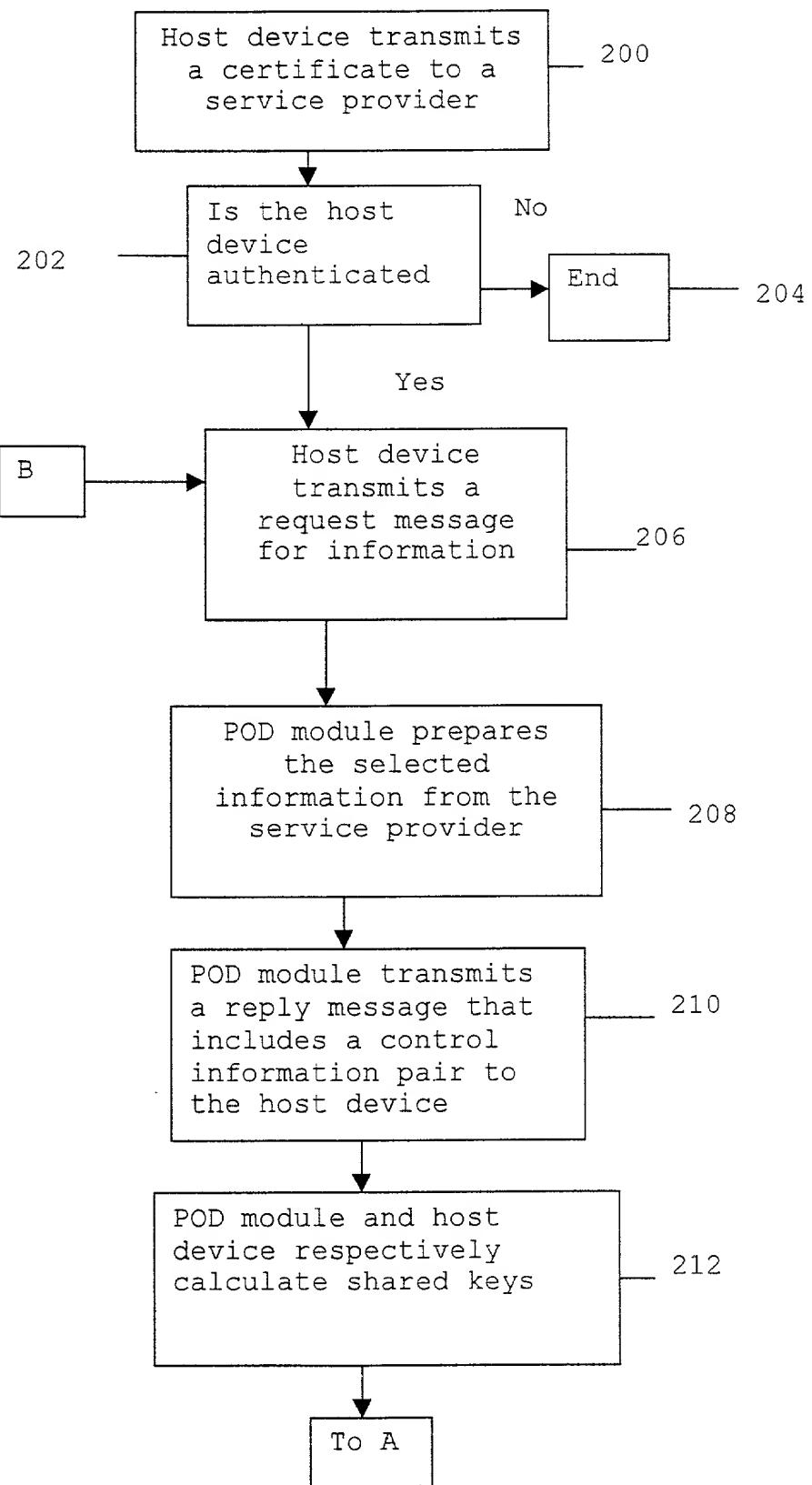
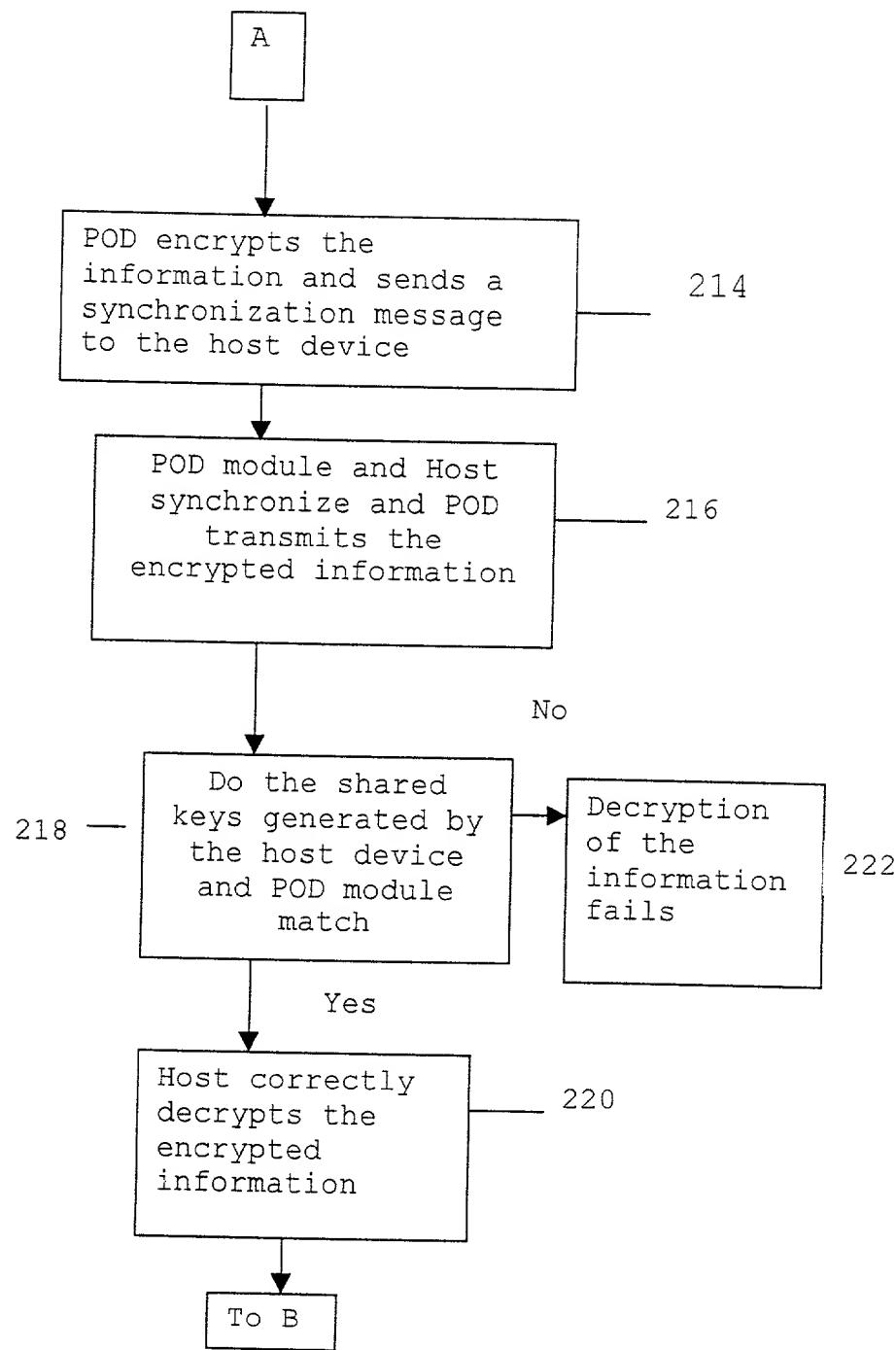


FIG. 2a

**FIG. 2b**

DECLARATION and POWER OF ATTORNEY

Attorney's Docket No. _____

700873

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **"SYSTEM AND METHOD FOR COPY PROTECTING TRANSMITTED INFORMATION"**

the specification of which (check one)

is attached hereto.

was filed on _____ as Application Serial No. _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by the amendment(s) referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulation, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

COUNTRY	APPLICATION NUMBER	DATE OF FILING (DAY, MONTH, YEAR)	PRIORITY CLAIMED UNDER 35 U.S.C. 119

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application (s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35 United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PRIOR UNITED STATES APPLICATION(S)

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (PATENTED, PENDING, ABANDONED)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Algy Tamoshunas, Reg. No. 27,677

Jack E. Haken, Reg. No. 26,902

SEND CORRESPONDENCE TO: Corporate Patent Counsel; U.S. Philips Corporation; 580 White Plains Road; Tarrytown, NY 10591	DIRECT TELEPHONE CALLS TO: (name and telephone No.) DANIEL J. PIOTROWSKI (914) 333-9624
--	---

Dated: <i>12/10/99</i>		INVENTOR'S SIGNATURE: <i>Jin Lu</i>		
Full Name of Inventor	Last Name LU	FIRST NAME JIN	Middle Name	
Residence & Citizenship	City W. CROTON-ON-HUDSON	STATE OR FOREIGN COUNTRY NEW YORK	Country of Citizenship CHINA	
Post Office Address	Street 107 SCENIC DRIVE	CITY W. CROTON-ON-HUDSON	State or Country NEW YORK	Zip Code 10520

Dated:		INVENTOR'S SIGNATURE:		
Full Name of Inventor	Last Name FREEMAN	FIRST NAME MARTIN	Middle Name	
Residence & Citizenship	City PALO ALTO	STATE OR FOREIGN COUNTRY CALIFORNIA	Country of Citizenship U.S.A.	
Post Office Address	Street 4189 DONALD DRIVE	CITY PALO ALTO	State or Country CALIFORNIA	Zip Code 94306

Dated:		INVENTOR'S SIGNATURE:		
Full Name of Inventor	Last Name	FIRST NAME	Middle Name	
Residence & Citizenship	City	STATE OR FOREIGN COUNTRY	Country of Citizenship	
Post Office Address	Street	CITY	State or Country	Zip Code

Dated:		INVENTOR'S SIGNATURE:		
Full Name of Inventor	Last Name	FIRST NAME	Middle Name	
Residence & Citizenship	City	STATE OR FOREIGN COUNTRY	Country of Citizenship	
Post Office Address	Street	CITY	State or Country	Zip Code

DECLARATION and POWER OF ATTORNEY

700873

Attorney's Docket No.
PHA 23,890

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **"SYSTEM AND METHOD FOR COPY PROTECTING TRANSMITTED INFORMATION"**

the specification of which (check one)

is attached hereto.

was filed on _____ as Application Serial No. _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by the amendment(s) referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulation, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

COUNTRY	APPLICATION NUMBER	DATE OF FILING (DAY, MONTH, YEAR)	PRIORITY CLAIMED UNDER 35 U.S.C. 119

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application (s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35 United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PRIOR UNITED STATES APPLICATION(S)

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (PATENTED, PENDING, ABANDONED)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Algy Tamoshunas, Reg. No. 27,677

Jack E. Haken, Reg. No. 26,902

SEND CORRESPONDENCE TO:
Corporate Patent Counsel;
U.S. Philips Corporation; 580 White Plains Road; Tarrytown, NY 10591

DIRECT TELEPHONE CALLS TO:
(name and telephone No.) DANIEL J. PIOTROWSKI
(914) 333-9624

Dated:		INVENTOR'S SIGNATURE:		
Full Name of Inventor	Last Name LU	FIRST NAME JIN	Middle Name	
Residence & Citizenship	City W. CROTON-ON-HUDSON	STATE OR FOREIGN COUNTRY NEW YORK	Country of Citizenship CHINA	
Post Office Address	Street 107 SCENIC DRIVE	CITY W. CROTON-ON-HUDSON	State or Country NEW YORK	Zip Code 10520

Dated. 12/10/99		INVENTOR'S SIGNATURE: <i>Martin Freeman</i>		
Full Name of Inventor	Last Name FREEMAN	FIRST NAME MARTIN	Middle Name	
Residence & Citizenship	City PALO ALTO	STATE OR FOREIGN COUNTRY CALIFORNIA	Country of Citizenship U.S.A.	
Post Office Address	Street 4189 DONALD DRIVE	CITY PALO ALTO	State or Country CALIFORNIA	Zip Code 94306

Dated:		INVENTOR'S SIGNATURE:		
Full Name of Inventor	Last Name	FIRST NAME	Middle Name	
Residence & Citizenship	City	STATE OR FOREIGN COUNTRY	Country of Citizenship	
Post Office Address	Street	CITY	State or Country	Zip Code

Dated:		INVENTOR'S SIGNATURE:		
Full Name of Inventor	Last Name	FIRST NAME	Middle Name	
Residence & Citizenship	City	STATE OR FOREIGN COUNTRY	Country of Citizenship	
Post Office Address	Street	CITY	State or Country	Zip Code

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Atty. Docket

JIN LU ET AL

PHA 23,890

Serial No.

Group Art Unit:

Filed: CONCURRENTLY

Examiner:

SYSTEM AND METHOD FOR COPY PROTECTING TRANSMITTED INFORMATION

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

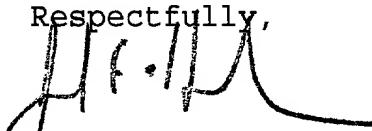
APPOINTMENT OF ASSOCIATES

Sir:

The undersigned Attorney of Record hereby revokes all prior appointments (if any) of Associate Attorney(s) or Agent(s) in the above-captioned case and appoints:

DANIEL J. PIOTROWSKI **(Registration No. 42,079)**
c/o U.S. PHILIPS CORPORATION, Intellectual Property Department, 580 White Plains Road, Tarrytown, New York 10591, his Associate Attorney(s)/Agent(s) with all the usual powers to prosecute the above-identified application and any division or continuation thereof, to make alterations and amendments therein, and to transact all business in the Patent and Trademark Office connected therewith.

ALL CORRESPONDENCE CONCERNING THIS APPLICATION AND THE LETTERS PATENT WHEN GRANTED SHOULD BE ADDRESSED TO THE UNDERSIGNED ATTORNEY OF RECORD.

Respectfully,


Jack E. Haken, Reg. 26,902
Attorney of Record

Dated at Tarrytown, New York
this 9TH day of DECEMBER, 1999

C:\USAPPS\APPASOC.PW